5 Best Practices for Remaining Malware-Free

Your bottom line depends on a secure network.

August 13, 2019 4 min read

Opinions expressed by *Entrepreneur* contributors are their own.

Nowadays, a large portion your work is likely done online. From keeping accounts and other records to interacting with your customers and marketing to get new ones, you're going to be relying a whole lot on your office's network. And when it comes to efficient data storage and processing, as well as lead generation, sales and generally increased profits, the most important thing you can do is secure that network. Here are a few tips to help.

1.Encrypt all access points with complex passwords.

The very worst thing you can do is leave devices running on the manufacturers' default passwords, which are widely known to hackers. Create new, complex passwords for all your access points by using phrases that have no connection to your business. If you're worried about forgetting them, you can use password managers such as LastPass. In addition, be sure to train your staff on password security and how to recognize phishing attempts.

Related: 4 Signs Your Site Traffic is Being Hijacked

2. Ensure your antivirus software is up to date.

There’s no point having antivirus software if its abilities to recognize and tackle malware aren’t up to date. New viruses are constantly being unleasged, and it’s essential that your network is safeguarded. Depending on which particular devices and software you are using, the process will be slightly different, but check for new definitions and update them regularly.

While you’re at it, go through your antivirus’ settings routinely to see if everything is optimized. Set a schedule for scans, and be sure to check the results for any files that might be posing problems.

3. Confine file-sharing to a single server.

The more devices that have file sharing enabled on your network, the more vulnerable it’ll be to intruders. The best solution is have a single, secure server for that purpose. That way, You can easily monitor for unauthorized access. It might be necessary to connect other computers to your file server directly at some point, or you might need to host some files on another computer in the short term. In either case, make sure it’s only temporary and that a professional guides you on how to do it safely.

Related: For the Average Hacker, Your Small Business is an Ideal Target

4. Have multiple backups and update

them regularly.

Realizing that you've lost important data is one of the worst feelings you can have as a business owner. In my experience, I've learned that adequate documentation is one of the most crucial aspects of management. Having to start over without records, contracts and other important files will put your business at a serious disadvantage. But with the right back up system in place – i.e. a combination of physical backup and cloud solution via Dropbox, Google Drive, Amazon or any similar product – you'll be able to prevent that from occurring. Be sure that you set up the permissions in your cloud storage well, giving read/write permissions on specific sets of documents only to those who need them. That way, you'll reduce the risk of unilateral tampering.

5. Obtain private IP addresses.

If your business uses Dynamic Host Configuration Protocol, or DHCP, consider making the shift to private IP addresses. The change will secure your network by assigning specific IP addresses to devices and making it easy to identify when an unauthorized device has connected to your network by checking your router logs.

Being able to immediately identify and tackle any malicious network intrusion can mean the difference between preventing a major breach and having your customer data sold on the dark web. And one wants to have their entire business held captive by the next WannaCry.

https://www.entrepreneur.com/article/335304